What is claimed is:

## CLAIMS

1. A method of providing cryptographic parameters for use in cryptographic applications in response to requests therefor, comprising the steps of:

pre-computing one or more different types of sets of cryptographic parameters, each said type of set being adapted for use by an associated type of cryptographic application;

securely storing said pre-computed sets of cryptographic parameters in a memory storage unit;

receiving a request for a set of cryptographic parameters having specified characteristics for use in a particular cryptographic application;

determining one of said sets of cryptographic parameters stored in said memory storage unit that has specified characteristics;

accessing said determined set of cryptographic parameters from said memory storage unit; and

providing said determined set of cryptographic parameters with minimal latency.

2. A method as recited in claim 1 wherein:

said step of pre-computing includes pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type including an associated number k of randomly generated distinct prime number values that are suitable for use in an associated type of cryptographic application, wherein $k \geq 1$; and

said step of receiving includes receiving a request specifying characteristics including a specified number of requested prime number values.

3. A method as recited in claim 1 wherein:

said step of pre-computing includes pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type including an associated number k of randomly generated distinct prime number values that are suitable for use in an associated type of cryptographic application, wherein $k \geq 1$, and wherein each of said prime number values has an associated length; and

said step of receiving includes receiving a request specifying characteristics including a specified number of requested prime number values and an associated specified length of each of said requested prime number values.

4. A method as recited in claim 1 wherein:

said step of pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type including an associated modulus n having an associated length L, each said modulus n being a composite number generated from the product of an associated number k of randomly generated distinct prime number values $p_1, p_2, \ldots p_k$, wherein $k \geq 2$; and

said step of receiving includes receiving a request specifying characteristics including a specified length of a requested modulus and a specified number of prime number values constituting prime factors of said requested modulus.

5. A method as recited in claim 4 wherein:

said step of pre-computing includes pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type further including an associated public key exponent value e; and

said step of receiving includes receiving a request specifying characteristics further including a specified public key exponent value.

6. A method as recited in claim 5 wherein said step of pre-computing includes pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type further including an associated private exponent value d determined based on said associated prime number values $p_1, p_2, \ldots p_k$ and said associated public key exponent value e.

7. A method as recited in claim 6 wherein said step of pre-computing includes pre-computing a plurality of different one or more types of sets of cryptographic parameters, each said set of an associated type further including a set of sub-task private exponents

$d_1, d_2, \ldots d_k$ pre-computed based on the associated prime number values $p_1, p_2, \ldots p_k$ and also based on the associated private exponent value d

8. A method as recited in claim 4 wherein said step of pre-computing includes pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type further including at least one set of Chinese Remainder Algorithm coefficients pre-computed based on said k associated prime number values prime number values $p_1, p_2, \ldots p_k$; and

said step of receiving includes receiving a request specifying characteristics further including a specified type of Chinese Remainder Algorithm.

9. A method as recited in claim 8 wherein said at least one set of set of Chinese Remainder Algorithm coefficients includes a first set of coefficients that may be used in a summation type of Chinese Remainder Algorithm, and a second set of coefficients that may be used in an iterative type of Chinese Remainder Algorithm.

10. A method as recited in claim 1 wherein each said set of parameters includes an associated number k of randomly generated prime numbers, wherein $k \geq 1$, and wherein said step of pre-computing is performed by a processing unit and a plurality of exponentiation units communicatively coupled with the processing unit, said step of pre-computing including:

randomly generating a plurality of k random odd numbers each being a prime number candidate; and

performing at least one probabilistic primality test on each of said candidates, each of said primality tests including an associated exponentiation operation executed by an associated one of the exponentiation units, said exponentiation operations being performed by said associated exponentiation units in parallel.

11. A method as recited in claim 1 wherein each said set of parameters includes an associated number k of randomly generated prime numbers, wherein $k \geq 1$, and wherein said step of pre-computing is performed by a processing unit and a plurality of

exponentiation units communicatively coupled with the processing unit, said step of pre-computing including:

randomly generating at least one random odd number providing a prime number candidate;

determining a plurality of **y** additional odd numbers based on said at least one randomly generated odd number to provide **y** additional prime number candidates, thereby providing a total number of **y+1** candidates; and

performing at least one probabilistic primality test on each of said **y+1** candidates, each of the **y+1** primality tests including an associated exponentiation operation executed by an associated one of **y+1** of the exponentiation units, said **y+1** exponentiation operations being performed by said associated **y+1** exponentiation units in parallel.

12. A method as recited in claim 11 wherein each said randomly generated odd number provides a random seed, and wherein said step of pre-computing further includes the step of determining only one prime number value based on each said random seed so that successive prime numbers are not determined by multiple performances of said step of pre-computing.

13. A method as recited in claim 1 wherein said step of securely storing said pre-computed cryptographic parameters in a memory storage unit further includes storing at least a portion of said cryptographic parameters in a first memory unit that is protected within a logical and physical security boundary.

14. A method as recited in claim 13 wherein said step of securely storing said cryptographic parameters in a memory storage unit further includes:

encrypting at least one of said cryptographic parameters using a cryptographic key;

storing said cryptographic key in said first memory unit located within said security boundary; and

storing said encrypted cryptographic parameters in a second memory unit located outside of said security boundary.

15. A method as recited in claim 14 wherein said step of accessing includes:

accessing said encrypted cryptographic parameters from said second memory unit;

accessing said cryptographic key from said first memory unit; and

decrypting said accessed cryptographic parameters using said accessed cryptographic key.

16. A method of providing cryptographic parameters for use in cryptographic applications in response to requests therefor, comprising the steps of:

pre-computing one or more different types of sets of cryptographic parameters, each said type of set being adapted for use by an associated type of cryptographic application using an associated public key exponent value e, each said set of an associated type including,

an associated modulus n having an associated length L and being a composite number generated from the product of an associated number k of randomly generated distinct and suitable prime number values $p_1, p_2, \ldots p_k$, wherein $k \geq 1$,

an associated public key exponent value e,

an associated private key exponent value d determined based on the associated prime number values $p_1, p_2, \ldots p_k$ and the associated public key exponent value e,

a set of sub-task private exponents $d_1, d_2, \ldots d_k$ that are pre-computed based on the associated prime number values $p_1, p_2, \ldots p_k$ and the associated private key exponent value d, and

at least one set of Chinese Remainder Algorithm coefficients pre-computed based on said associated prime number values $p_1, p_2, \ldots p_k$;

securely storing said different types of sets of cryptographic parameters in a memory storage unit;

receiving a request for a specified type of set of cryptographic parameters having specified characteristics for use in a particular cryptographic application, said specified characteristics including,

a specified length L of a requested modulus N that is to be a composite number generated as a product of an associated specified number of prime number values,

a specified public key exponent value e, and

a specified type of Chinese Remainder Algorithm being used by the particular cryptographic application;

determining one of said sets of cryptographic parameters stored in said memory storage unit that has said specified characteristics;

accessing said determined set of cryptographic parameters from said memory storage unit; and

providing said determined set of cryptographic parameters with minimal latency.

17. A method for providing prime number values with minimal latency in response to requests therefor, comprising the steps of:

pre-computing a plurality of random distinct prime number values that are suitable for use in a cryptographic security application;

securely storing said pre-computed prime number values in a memory storage unit;

receiving a request for at least one prime number value to be used in a particular cryptographic application;

accessing at least one of said securely stored prime number values from said memory storage unit; and

providing said at least one accessed prime number value with minimal latency in response to said request.

18. A method as recited in claim 17 wherein:

said step of pre-computing includes pre-computing a plurality of random distinct prime number values having different associated lengths;

said step of receiving a request further includes receiving information indicating an associated specified length for at least one of said prime number values; and

said step of accessing includes,

determining at least one of said securely stored prime number values that has said associated specified length, and

accessing said at least one determined prime number value from said memory storage unit.

19. A method as recited in claim 17 wherein said step of receiving a request further includes receiving information indicating a specified number of requested prime number values.

20. A system for providing cryptographic parameters for use in cryptographic applications in response to requests therefor, comprising:

means for pre-computing one or more different types of sets of cryptographic parameters, each said type of set being adapted for use by an associated type of cryptographic application;

memory storage means for securely storing said pre-computed sets of cryptographic parameters;

means for receiving a request for a set of cryptographic parameters having specified characteristics for use in a particular cryptographic application;

means for determining one of said sets of cryptographic parameters stored in said memory storage unit that has specified characteristics;

means for accessing said determined set of cryptographic parameters from said memory storage unit; and

means for providing said determined set of cryptographic parameters with minimal latency.

21. A system as recited in claim 20 wherein:

said means for pre-computing is operative to pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type including an

associated number k of randomly generated distinct prime number values that are suitable for use in an associated type of cryptographic application, wherein $k \geq 1$; and

said means for receiving is responsive to a request specifying characteristics including a specified number of requested prime number values.

22. A system as recited in claim 20 wherein:

said means for pre-computing is operative to pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type including an associated number k of randomly generated distinct prime number values that are suitable for use in an associated type of cryptographic application, wherein $k \geq 1$, and wherein each of said prime number value has an associated length; and

said means for receiving is responsive to a request specifying characteristics including a specified number of requested prime number values and an associated specified length of each of said requested prime number values.

23. A system as recited in claim 20 wherein:

said means for pre-computing is operative to pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type including an associated modulus n having an associated length L, each said modulus n being a composite number generated from the product of an associated number k of randomly generated distinct prime number values $p_1, p_2, \ldots p_k$, wherein $k \geq 2$; and

said means for receiving is responsive to a request specifying characteristics including a specified length of a requested modulus and a specified number of prime number values constituting prime factors of said requested modulus.

24. A system as recited in claim 23 wherein said means for pre-computing is operative to pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type further including an associated public key exponent value e; and

said means for receiving is responsive to a request specifying characteristics further including a specified public key exponent value.

25. A system as recited in claim 24 wherein said means for pre-computing is operative to pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type further including an associated private exponent value d determined based on said associated prime number values $p_1$, $p_2$, ... $p_k$ and said associated public key exponent value e.

26. A system as recited in claim 25 wherein said means for pre-computing is operative to pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type further including a set of sub-task private exponents $d_1$, $d_2$, ... $d_k$ pre-computed based on the associated prime number values $p_1$, $p_2$, ... $p_k$ and also based on said associated private exponent value d.

27. A system as recited in claim 23 wherein:

said means for pre-computing is operative to pre-computing one or more different types of sets of cryptographic parameters, each said set of an associated type further including at least one set of Chinese Remainder Algorithm coefficients pre-computed based on said associated prime number values $p_1$, $p_2$, ... $p_k$; and

said means for receiving is responsive to a request specifying characteristics further including a specified type of Chinese Remainder Algorithm.

28. A system as recited in claim 27 wherein said at least one set of set of Chinese Remainder Algorithm coefficients includes a first set of coefficients that may be used in a summation type of Chinese Remainder Algorithm, and a second set of coefficients that may be used in an iterative type of Chinese Remainder Algorithm

29. A system as recited in claim 22 wherein said means for pre-computing includes a prime number generation unit for randomly generating said prime numbers.

30. A system as recited in claim 29 wherein said prime number generation unit provides for searching in parallel for a plurality of prime number values simultaneously, said prime number generation unit including:

processing means operative to randomly generate a random odd number providing a prime number candidate, and to provide a set of test parameters associated with a probabilistic primality test to be performed on each said randomly generated number, each said set of said test parameters including said associated randomly generated number; and

at least one exponentiation unit being communicatively coupled with said processing means, and being responsive to said set of test parameters, and operative to perform an exponentiation operation based on said set of test parameters and an associated base value, and also operative to generate a primality test result signal declaring said prime number candidate to be either composite or prime with reference to said associated base value;

said processing means being responsive to said primality test result signal, and operative to process said test result signal for the purpose of eliminating randomly generated numbers declared to be composite in accordance with a search for prime number values.

31. A system as recited in claim 29 wherein said prime number generation unit provides for searching in parallel for a plurality of prime number values simultaneously, said prime number generation unit including:

processing means operative to randomly generate a plurality of k random odd numbers each providing a prime number candidate, and to provide at least one set of test parameters associated with a probabilistic primality test to be performed on each one of said plurality of k randomly generated numbers, each said set of said test parameters including said associated randomly generated number and an associated base value; and

a plurality of exponentiation units each being communicatively coupled with said processing means, and being responsive to an associated one of said sets of test parameters, and operative to perform an exponentiation operation based on said associated set of test parameters, and also operative to generate a primality test result

signal declaring said associated prime number candidate to be either composite or prime with reference to said associated base value, said exponentiation units being operative to perform said exponentiation operations in parallel;

said processing means being responsive to said primality test result signals, and operative to process said test result signals for the purpose of eliminating randomly generated numbers declared to be composite in accordance with a search for prime number values.

32. A system as recited in claim 29 wherein said prime number generation unit provides for searching in parallel for a plurality of prime number values simultaneously, said prime number generation unit including:

processing means operative to randomly generate at least one random odd number providing a prime number candidate, and to determine a plurality of y additional odd numbers based on each of said at least one randomly generated odd number to provide y additional prime number candidates, thereby providing a total number of y+1 candidates, said processing means also being operative to provide at least one set of test parameters associated with a probabilistic primality test to be performed on each one of said prime number candidates, each said set of test parameters including said associated prime number candidate and an associated base value; and

a plurality of exponentiation units each being communicatively coupled with said processing means, and being responsive to an associated one of said sets of test parameters, and operative to perform an exponentiation operation based on said associated set of test parameters, and also operative to generate a primality test result signal declaring said associated prime number candidate to be either composite or prime with reference to said associated base value, said exponentiation units being operative to perform said exponentiation operations in parallel;

said processing means being responsive to said primality test result signals, and operative to process said test result signals for the purpose of eliminating randomly generated numbers declared to be composite in accordance with a search for prime number values.

33. A system as recited in claim 32 wherein each said randomly generated odd number provides a random seed, and wherein said processing means is further operative to determine only one prime number value for each said random seed so that said prime number generation unit does not generate successive primes.

34. A system as recited in claim 29 wherein said prime number generation unit is configured to be protected within a logical and physical security boundary.

35. A system as recited in claim 34 wherein said storage means includes a first memory unit located within said security boundary of said prime number generation unit.

36. A system as recited in claim 35 wherein:

said storage means further includes a second memory unit located outside of said security boundary; and

said prime number generation unit includes means for encrypting a pre-computed prime number using a cryptographic key, storing said cryptographic key in said first memory unit located within said security boundary, and storing the encrypted prime number in said second memory unit located outside of said security boundary.

37. A system as recited in claim 36 wherein said second memory unit is a database.

38. A server system operative to pre-compute prime numbers and securely store the pre-computed prime numbers for later use, comprising:

a server computing system communicatively coupled with a plurality of remote clients via a network, and being responsive to requests for randomly generated prime numbers each being associated with ones of said remote clients;

a prime number generation unit communicatively coupled with said server computing system and providing for pre-computing a plurality of randomly generated prime numbers, said prime number generation unit being configured to be protected within a logical and physical security boundary; and

a secure memory unit protected within said security boundary and being communicatively coupled with said server computing system and said prime number generation unit, said secure memory unit providing for storage of said pre-computed prime numbers;

said server computing system being operative to access said prime numbers stored in said secure memory unit, and to provide said prime numbers with minimal latency in response to said requests for randomly generated prime numbers.

39. A server system as recited in claims 38 further comprising:

an unsecure memory unit located outside of said security boundary and being communicatively coupled with said server computing system and said prime number generation unit, said unsecure memory unit also providing for storage of pre-computed prime numbers; and

means for encrypting a pre-computed prime number using a cryptographic key, for storing said cryptographic key in said secure memory unit protected within said security boundary, and for storing the encrypted prime number in said unsecure memory unit located outside of said security boundary;

said server computing system being further operative to access said encrypted prime number stored in said unsecure memory unit, to access said cryptographic key from said secure memory unit, to decrypt said accessed prime number using said cryptographic key, and to provide said decrypted prime number with minimal latency in response to one of said requests for a randomly generated prime number.

40. A server system for processing cryptographic transactions and for providing prime number values in response to user requests therefor, comprising:

a server computing system operative communicatively coupled with a plurality of remote clients via a network, and including a queuing means for storing a plurality of queued job requests including cryptographic transaction job requests, and prime number requests having associated length parameters specifying a length for a randomly generated prime number, said server computing system being operative to determine a

number of prime number requests and a number of transaction job requests currently stored in said queuing means;

a cryptographic processing unit communicatively coupled with said server computing system, and being operative to search for randomly generated prime numbers and to process cryptographic transactions in response to requests therefor;

at least one exponentiation unit communicatively coupled with said cryptographic processing unit and providing exponentiation resources for use in searching for randomly generated prime numbers and in processing cryptographic transactions; and

a storage means communicatively coupled with said cryptographic unit for storing said randomly generated prime numbers;

said cryptographic unit also being operative to perform the steps of,

determining a number of pre-computed prime numbers currently stored in the local secure memory unit;

based on the number of prime number requests and cryptographic transaction job requests currently stored in the queuing unit, and the number of cryptographic key values currently stored in the storage unit, dynamically allocating a first portion of said exponentiation resources for prime number searching, and a second portion of the total exponentiation resources for processing cryptographic transactions,

performing prime number searching functions in response to said prime number requests and associated length parameters, said number searching functions including randomly generating at least one random odd number having the specified length, and performing at least one probabilistic primality test on said random number, each of said primality tests including an associated exponentiation operation executed using said first dynamically allocated portion of the said exponentiation resources, and

performing cryptographic transaction processing functions in response to said cryptographic transaction job requests using said second dynamically allocated portion of said exponentiation resources.

41. A server system as recited in claim 40 wherein said cryptographic unit is operative to perform said step of determining said first and second dynamically allocated portions of said exponentiation resources by performing the further steps of:

determining whether said number of stored prime number values is less than a predetermined number; and

if the number of stored prime numbers is less than a predetermined number, dynamically increasing said first portion of said exponentiation resources allocated for prime number generating.

42. In a server system for processing cryptographic transactions and for providing randomly generated prime numbers in response to requests therefor, the server system including a computing system operative to communicate with a plurality of remote clients via a network, a memory storage unit for storing said randomly generated prime numbers, a queuing unit for storing a plurality of queued job requests including cryptographic transaction job requests, and prime number requests having associated length parameters specifying a length for a randomly generated prime number to be provided, and at least one exponentiation unit communicatively coupled with said cryptographic unit and providing exponentiation resources for use in searching for randomly generated prime numbers and in processing cryptographic transactions, a process of dynamically allocating portions of said exponentiation resources for processing cryptographic transactions and for searching for randomly generated prime numbers, comprising the steps of:

determining a number of prime number requests and a number of cryptographic transaction job requests currently stored in the queuing unit;

determining a number of pre-computed prime numbers currently stored in the memory unit; and

based on said number of prime number requests and said number of cryptographic transaction job requests currently stored in the queuing unit, and said number of prime numbers currently stored in the memory unit, determining portions of said exponentiation resources to be dynamically allocated for prime number searching, and for processing cryptographic transactions .

43. In a server system for processing cryptographic transactions and for providing randomly generated prime numbers in response to requests therefor, the server system including a computing system operative to communicate with a plurality of remote clients via a network, a memory storage unit for storing said randomly generated prime numbers, a queuing unit for storing a plurality of queued job requests including cryptographic transaction job requests, and prime number requests having associated length parameters specifying a length for a randomly generated prime number to be provided, and at least one exponentiation unit communicatively coupled with said cryptographic unit and providing exponentiation resources for use in searching for randomly generated prime numbers and in processing cryptographic transactions, a software system for dynamically allocating portions of said exponentiation resources for processing cryptographic transactions and for searching for randomly generated prime numbers, comprising:

a first module for determining a number of prime number requests and a number of cryptographic transaction job requests currently stored in the queuing unit;

a second module operative to determine a number of pre-computed prime numbers currently stored in the memory unit;

a third module operative to determine a portion of said exponentiation resources to be dynamically allocated for prime number searching, and a portion of said exponentiation resources to be dynamically allocated for processing cryptographic transactions based on said number of prime number requests and said number of cryptographic transaction job requests currently stored in the queuing unit, and based on said number of prime numbers currently stored in the memory unit;

a fourth module operative to perform prime number searching functions in response to said prime number requests and associated length parameters, said number searching functions including randomly generating at least one random odd number having the specified length, and performing at least one probabilistic primality test on said random number, each of said primality tests including an associated exponentiation operation executed using said first dynamically allocated portion of the said exponentiation resources; and

a fifth module operative to perform cryptographic transaction processing functions in response to said cryptographic transaction job requests using said second dynamically allocated portion of said exponentiation resources.